

selected value of  $N$ , [and]  $N$  number of tokens and a second checksum value to be used to authenticate the sender [receiver] computer;

each of the additional transmissions being variable and adaptively selected, at least in part, based upon a set of criteria [that are] used in an algorithm to determine the number of additional transmissions, the criteria being selected from a group consisting of the frequency of transmissions between the sender computer and the receiver computer, the closeness of the sender computer to the source of the transactions, and the usage patterns of the sender computer.

### **REMARKS**

Reconsideration of this Application is respectfully requested. Independent claims 1, 14 and 23 are amended, without prejudice or disclaimer. Claims 1-17, 19, 20, 22 and 23 are in this case.

Initially, in response to the Applicants' amendments and arguments set forth in the Amendment dated December 30, 2003, the Examiner recommended that, when constructing claims 1, 14 and 23, Applicants follow the authentication steps in the Specification on page 24, lines 5-14; page 25, lines 1-9; and page 27, line 19-page 29, line 8 (i.e., "Client usage patterns"). The Examiner indicated that, such clearly details the process steps that claims 1, 14 and 23 seek to model, including the particulars on pages 27-29 of when  $N$  is a variable.

The Examiner then rejected claims 1-17, 19, 20, 22 and 23 under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement. Specifically, the Examiner takes the position that, while claims 1, 14 and 23 recite the trans-

mission of a “selected value of N”, the claims also recite the limitation of “the number of tokens being set to a variable N”. The Examiner explains that to one of ordinary skill the term “selected value of N” means a client transmitting to a server a “subset” of the N number of tokens. The Specification, however, according to the Examiner, recites a client informing a server the value of N and transmitting N tokens for future authentication (Specification, amended page 28). The Examiner notes that claims 2-13 and 15-19, 20 and 22 are rejected as they depend from claims 1 and 14, respectively.

The Examiner also rejected claims 1-17, 19, 20, 22 and 23 under 35 U.S.C. § 112, second paragraph, for indefiniteness. More particularly, the Examiner asserts that claims 1, 14 and 23 recite conflicting steps regarding what actions are to be performed by a client during a “first secure transmission”. The Examiner believes that it is not clear whether Applicants, in the step of transmitting “a selected value of N and N number of tokens to be used to authenticate the sender computer” is referring to a subsequent “first secure transmissions” or just the one “first secure transmission” detailed in the first three steps of each of claims 1, 14 and 23. The Examiner notes that claims 2-13 and 15-19, 20 and 22 are similarly rejected as they depend from claims 1 and 14, respectively.

Additionally, the Examiner rejected claims 1, 14 and 23 under 35 U.S.C. § 112, second, paragraph, as allegedly being incomplete for omitting essential steps, such omission amounting to a gap between the steps (citing MPEP § 2172.01). The Examiner states that the omitted steps are: Where the number N defines the number of additional transmissions. The Examiner reiterates that claims 2-13 and 15-19, 20 and 22 are rejected as they depend from claims 1 and 14, respectively.

Claims 1, 14 and 23 are amended, accordingly, to delineate that, in the step of transmitting “a selected value of N and N number of tokens to be used to authenticate the sender computer”, Applicants are referring to subsequent “first secure transmissions”, namely, a “second secure transmission during which the sender computer transmits to the receiver computer a second selected value of N, N number of tokens and a second checksum value to be used to authenticate the sender computer”. The claims are also amended to clarify that where the number of tokens are set to a variable N, N defines a selected number of additional transmissions and each token is a unique identifier. Applicants voluntarily add the language “, the method” to the preamble of the claims to better define the invention without limiting effect.

Withdrawal of the Examiner’s rejections under § 112, first and second paragraphs, is, therefore, respectfully requested.

\* \* \* \* \*

Next, the Examiner rejected claims 1-3, 6-11, 14 and 15 under 35 U.S.C. § 102(e) as being anticipated by Pickett, U.S. Patent No. 6,012,144. According to the Examiner, Pickett teaches a transaction security method and apparatus comprising the following steps: (i) transmitting a token to a receiver during first secure transmission between a sender and a receiver (Abstract; Figure 4; and column 3, lines 50-52); (ii) establishing at least one additional transmission between the sender and receiver for transmitting the token, wherein the additional transmission is variable and adaptively selected (Figures 4 and 5; column 3, lines 50-54; and column 6, lines 22-35); (iii) comparing the tokens received during the trans-

mission to establish authenticity (Figures 4 and 5; column 6, lines 23-35 and 64-67); (iv) wherein the at least one token comprises and corresponds to a preselected number of tokens (Figures 4 and 5); (v) conducting transmissions over unsecure or open connections (Figure 1); (vi) conducting an encrypted first secure transmission (Figures 3A-4; column 5, line 1 through column 6, line 23); and (vii) additional transmissions that are sent in plaintext (Figures 1 and 5; column 6, lines 22-35).

The Examiner also indicates that Pickett teaches a sender computer transmitting to a receiver computer a selected value of N and N number of tokens to be used to authenticate the sender computer (Figures 4 and 5) as, for the case of N=1, the user “informs” the server of the value of N by registering at least one token to be used for future purchases.

\* \* \* \* \*

In addition, the Examiner rejected claims 4, 5, 12, 13, 16, 17, 19, 20 and 22 under 35 U.S.C. § 103(a) as being obvious and, therefore, unpatentable over Pickett. More particularly, regarding claims 4, 5 and 22, the Examiner argues that Pickett teaches a secure transaction method that comprises multiple transmissions and the exchange of token data (Figures 4 and 5). While the Examiner acknowledges that Pickett does not specify a particular number of additional transmissions, he asserts that it would have been obvious for a user to register multiple cards but only make one purchase using the service of Pickett, or to register one card and make multiple purchases using the one card. Similarly, the Examiner continues, as the number of additional transactions of the Pickett system is variable, the number can be ascertained mathematically (i.e., deterministically), or at least statistically, or probabilistically. The Examiner states further that the choice of independent variables used

to model the behavior of said variable is at the discretion of the practitioner.

With respect to claims 12, 13, 16 and 17, the Examiner takes the position that Pickett teaches transmitting data electronically (Figures 1-5). The Examiner takes Official Notice that checksums are well known computational tools for detecting the presence of errors when data is transmitted over a network. The Examiner then concludes that it would have been obvious to one having ordinary skill in the art to use “checksums” to detect errors during the transmission of sensitive data such as credit card numbers.

As for claims 19 and 20, the Examiner has determined that Pickett teaches a secure transaction method that comprises additional transmissions to a client (Figure 5). With regard to the number of additional transmissions, the Examiner finds that it would have been obvious for a user to decline using the system of Pickett, or at least a particular website (i.e., ABC Toy Company), (Figure 5) in the future if the user was dissatisfied with the service.

\* \* \* \* \*

Finally, the Examiner rejected claim 23 under 35 U.S.C. § 103(a) as being obvious and, therefore, unpatentable over Pickett in view of Maher, U.S. Patent No. 6,125,349. The Examiner asserts that Pickett teaches a method and system for authenticating transferred data between a sender computer and a receiver computer comprising the following steps: (i) transmitting a token to a receiver during first secure transmission between a sender and a receiver (Abstract; Figure 4; and column 3, lines 50-52); (ii) establishing at least one additional transmission between the sender and receiver for transmitting the token, wherein the additional transmission is variable and adaptively selected (Figures 4 and 5; column 3, lines 50-54; and column 6, lines 22-35); (iii) comparing the tokens received during the trans-

missions to establish authenticity (Figures 4 and 5; column 6, lines 23-35 and 64-67); and (iv) wherein the at least one token comprises and corresponds to a preselected number of tokens sent during a first secure transmission (Figures 4 and 5).

The Examiner also indicates that Pickett teaches a sender computer transmitting to a receiver computer a selected value of N and N number of tokens to be used to authenticate the sender computer (Figures 4 and 5). The Examiner acknowledges that Pickett does not explicitly recite specific criteria as input in an algorithm to determine the number of additional transmissions. He then looks to Maher which, he says, teaches a system for authenticating transferred data between a sender computer and a receiver computer that uses an algorithm to determine additional transmissions based on frequency of transmissions between sender and receiver, proximity of the sender computer to the receiver computer or usage pattern of the sender (column 6, lines 25-48; column 7, lines 5-25). The Examiner concludes that it would have been obvious to one of ordinary skill in the art to combine the teachings of Pickett and Maher in order to increase usage of the system through a rewards program (column 7, lines 5-25).

\* \* \* \* \*

First, in accordance with the Examiner's recommendation, claims 1, 14 and 23 are amended to further incorporate the authentication steps and when N is a variable, as set forth generally in the Specification on pages 24, 25 and 27-29. Applicants reiterate that the claims define the number of tokens N and clarify that each time a first secure transmission is performed, the sender computer transmits to the receiver computer a selected value of N, N number of tokens, and a checksum value to be used to authenticate the sender computer.

Applicants emphasize, in this connection, their previous amendments to the Specification, set forth in the Amendment dated December 30, 2003. Such amendments from the first full paragraph on page 28 of the Specification through the first full paragraph on page 29 were made for purposes of clarification and consistency, namely, to clarify that the number of tokens N is a variable, and to substitute “N” for “M” throughout the Specification.

\* \* \* \* \*

As for the rejections under §§ 102(e) and 103(a), Applicants respectfully disagree with the Examiner’s reading and application of the cited references. Nevertheless, Applicants respectfully submit that Pickett’s description, “users of the security system 10 employ two different types of secure transactions. The first type is used to register the user’s credit card. The second type is used to make purchases using those registered credit cards” (column 3, lines 50-52), does not disclose or suggest Applicants’ amended claim step of “transmitting selected authentication information including at least one token and a checksum value from the sender computer to the receiver computer during the first secure transmission so as to allow the sender computer to authenticate itself, the number of tokens being set to a variable N where N defines a selected number of additional transmissions and each token is a unique identifier”.

Applicants also submit that their amended claim step of “comparing the at least one token transmitted from the sender computer during the additional transmission to each of the token(s) transmitted from the sender computer during the one or more previous transmission(s) to determine whether the most recent additional transmission is authentic” is neither disclosed nor is it suggested by the following language of Pickett (column 6, lines 23-

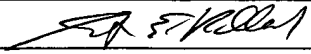
35): (i) "a second type of transaction occurs when the user wishes to make a purchase on the Internet...The user accesses a Web page 130 (FIG. 5) containing an order form for the product or service desired. That page accesses the computer system's Slice 0 computer which presents to him a list of credit cards he registered using the names he gave the cards when he registered...Once again, both slices are needed".


Neither Pickett nor Maher, we submit, whether taken alone or in any combination, disclose or suggest Applicants' authentication steps, a variable N as defined, nor the client computer usage patterns, as claimed by Applicants. Accordingly, withdrawal of the Examiner's rejections under §§ 102(e) and 103(a) is appropriate.

Applicants have made a good faith attempt to place this Application in condition for allowance. Favorable action is requested. If there is any further point requiring attention prior to allowance, the Examiner is asked to contact Applicants' counsel at (212) 768-3800. Please charge any additional fees that may be required to our firm Deposit Account No. 50-0518.

Respectfully submitted,

Dated: September 10, 2004

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, in an envelope with sufficient postage addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 10, 2004  
Name Grant E. Pollack  
  
Signature

  
Grant E. Pollack, Esq.  
Registration No. 34,097  
Steinberg & Raskin, P.C.  
1140 Avenue of the Americas, 15<sup>th</sup> Floor  
New York, New York 10036  
(212) 768-3800, Ext. 253  
Attorney for Applicants